REMARKS

These remarks follow the order of the paragraphs of the office action. Relevant portions of the office action are shown indented and italicized.

Applicants request a review of the 'FINAL' status of the office communication, in so much that it is not the applicants' amendment that caused any further search. Porras and only Porras was used in the previous office communication.

DETAILED ACTION

Response to Amendment

1. Applicant's amendments with respect to claims 1, 4, 7, 10 and new claims 19 and 20 filed 03/21/07 have been accepted. Therefore claims 1 - 20 are pending- The amendments however have introduced some claims objections.

Claim Objections

2 Claim 19 is objected to because of the following informalities: • Recitation of numeral 2 after introducing claim 19 as a new claim.
• Unnecessary usage of an open parenthesis at the end of the claim.
Appropriate correction is required.

In response, the applicants respectfully states that claim 19 is amended to overcome the claim objections.

Response to Arguments

3. Applicant's arguments filed 03/21/2007 have been fully considered but they are not persuasive. It is Applicant's primary assertions that Porras does not disclose monitoring in real time and does not use packet streams. The Examiner respectfully disagrees. Porras discloses real-time analysis of network packets as performed by service monitors (see column 3, lines 51 - 53). This analysis results in the statistical profiling of events streams (see column 5, lines 46 - 50). Furthermore, in response to applicants argument that Porras is based on statistics, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. It the prior art structure is capable of performing the intended use, then it meets the claim.

In particular, it is Applicant's argument that claim 1, Porras does not allude to "a communications sensor for receiving and monitoring in real time communications packets flowing at arbitrary points on a network. said communications being any of communications conducted via a host and communications conducted directly" or does not anticipate calculating formal similarity between two packet streams composed of communications packets entering the sensor upon arrival of the communications packets, and said sensor employing said formal similarity in detecting an intrusion." Again Porras discloses dynamic deployment of network monitors that are responsible for real time surveillance of a network (see column 3, lines 41 - 63). The short and long term statistical profiles aid in the generation of a statistical score that represents the similarities between the identified network packet streams that were subjected to network surveillance. (see column 5, lines 46 - 50; column 6, lines 20 - 23).

In response, the applicants respectfully states that exception is taken with the office communication statements in the above response to arguments. Firstly, Porras is based on building at least one long-term and a least one short-term statistical profile from a measure of the network packets that monitors data transfers, errors, or network connections. . A comparison of the statistical profiles is used to determine whether the difference between the statistical profiles indicates suspicious network activity. The invention claimed in claims 1-20 of the present application is not concerned with a comparison of anything long to anything short.

The office communication states above:

Porras discloses real-time analysis of network packets as performed by service monitors (see column 3, lines 51 - 53). This analysis results in the statistical profiling of events streams (see column 5, lines 46 - 50).

Porras's monitoring may be in real time but there is indication, reason to believe, or anticipation of "monitoring in real time communications packets flowing at arbitrary points on a network," as in claims 1-20.

The office communication states above:

Furthermore, in response to applicants argument that Porras is based on statistics, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. It the prior art structure is capable of performing the intended use, then it meets the claim.

Applicants take exception with the above statement in an anticipation rejection.. Anticipation requires having each and every element of the rejected claim, which Porras does not. Besides, Porras's structure is one that necessitates and employs apparatus and/or steps for developing and using statistics. Thus, Porras's structure indeed is not "capable of performing the intended use," of claims 1-20 based on packet comparison of streams to obtain 'formal similarity' as defined in the present specification.

The office communication states above:

> *Again Porras discloses dynamic deployment of network monitors that are responsible for real time surveillance of a network (see column 3, lines 41 - 63). The short and long term statistical profiles aid in the generation of a statistical score that represents the similarities between the identified network packet streams that were subjected to network surveillance. (see column 5, lines 46 - 50; column 6, lines 20 - 23).*

This office communication statement gives some indication of what Porras does. It appears to be a clear admission that Porras does not teach claim 1. Claim 1 has nothing to do with:

comparison of short and long term anything;

statistical profiles of anything;

generation any statistical score;

any statistical similarities between packet streams;

any network surveillance, short and long term statistical profiles; or

aid in the generation of a statistical score that represents the similarities between the identified network packet streams that were subjected to network surveillance.

Applicants still maintain arguments the office communication somewhat reproduced above:

> *In particular, it is Applicant's argument that claim 1, Porras does not allude to "a communications sensor for receiving and monitoring in real time communications packets flowing at arbitrary points on a network. said communications being any of communications conducted via a host and communications conducted directly" or does not anticipate calculating formal similarity between two packet streams composed of communications packets entering the sensor upon arrival of the communications packets, and said sensor employing said formal similarity in detecting an intrusion."*

Applicants still maintain Porras does not teach or anticipate:

doing anything at arbitrary points on a network.

receiving and monitoring in real time communications packets flowing at arbitrary points on a network.

communications being any of communications conducted via a host and communications conducted directly;

\ calculating formal similarity between anything;

calculating formal similarity between two packet streams composed of communications packets entering the sensor upon arrival of the communications packets;

employing said formal similarity for anything; or

employing said formal similarity in detecting an intrusion.

Thus, applicants' previous remarks stand.

As for claim 2, it is Applicant's assertion that Porras does not anticipate Claim 2's limitation in regard to "two packet streams by graphs depicting amounts of data in communications packets in respective packet streams with respect to elapsed time, and calculates similarity between the two packet streams. Porras teaches surveillance of event streams which are derived of network packet observation and collection (see column 1, lines 51 - 53). Moreover, the short and long term profiles of Porras are equivalent to the graphs depicting data communications since the profiles consist of data communication information (see column 1, lines 53 - 61; column 2, lines 49-60). The functionality and purpose of the profiles are parallel to those of the graphs as taught in Applicant's claimed invention.

Applicant has presents similar arguments to those addressed in respect to claims 1 and 2 and therefore the rejections of these claims are maintained for similar reasons.

In response, the applicants respectfully states that exception is taken with the so called equivalence of Porras's profiles to graphs.

The office communication states above:

Porras teaches surveillance of event streams which are derived of network packet observation and collection (see column 1, lines 51 - 53). Moreover, the short and long term profiles of Porras are equivalent to the graphs depicting data communications since the profiles consist of data communication information (see column 1, lines 53 - 61; column 2, lines 49-60).

Indeed. a review of the office communication's statement of Porras's "network packet observation and collection (see column 1, lines 51 - 53)" have no teaching of the elements of claim 2.

The further statement, "[M]oreover, the short and long term profiles of Porras are equivalent to the graphs depicting data communications since the profiles consist of data communication information (see column 1, lines 53 - 61; column 2, lines 49-60), is extremely not understood and traversed by the applicants. There is no such equivalence. Porras's profiles, not being graphic cannot be teaching any part of claim 2, and certainly not "calculates similarity between the two packet streams based on size of regions enclosed by the two graphs when the graphs of the packet streams are moved close to each other without intersecting each other." How do profiles move close to each other without intersecting each other?" Thus, the applicants' remarks in previous responses to claim 2 still stand.

Indeed exception is taken with the office communication statement:

> *The functionality and purpose of the profiles are parallel to those of the graphs as taught in Applicant's claimed invention.*

There is indeed no similarity or parallel teaching in Porras and the graph of claim 2.

Exception is also taken with the office communication statement:

> *Applicant has presents similar arguments to those addressed in respect to claims 1 and 2 and therefore the rejections of these claims are maintained for similar reasons.*

Indeed, it is unfortunate that the office communication does not address all the remaining arguments made previously for the remaining claims. However, as with claims 1 and 2, applicants' previous remarks stand.

> ***Claim Rejections - 35 USC § 102***
>
> *The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:*
>
> *A person shall be entitled to a patent unless -*
>
> *(a) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention Thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.*
>
> *The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA). and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore,*

the prior art date of the reference is determined under 35 USC: 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4. Claims 1 - 20 are rejected under 36 U.S.C. 102(e) as being anticipated by Porras et al. in US Patent No. 6711615 (hereinafter US 615).

In response, the applicant respectfully states that Claims 1-20 are apparently not anticipated by the invention of Porras. The present invention, claimed in Claims 1-20, provides:

"Systems, apparatus and methods to monitor communications conducted via a host computer placed under the management of security measures such as firewalls or routers' filtering capabilities. A communications monitoring system which includes a packet input means for connecting to predetermined points on a network via a network interface and receiving communications packets flowing at the points; and matching means for performing real-time matching between two packet streams composed of received communications packets each time a communications packet is received. If the two packet streams are highly similar, it is highly likely that an attack or intrusion is being made and an alert is issued."

Thus the invention claimed in claims 1-20 are concerned with "performing real-time matching between two packet streams composed of received communications packets each time a communications packet is received."

Whereas, the cited art to Porras, US Patent 6,711,615, filed: September 25, 2002, is entitled: "Network surveillance". The Porras abstract reads:

"A method of network surveillance includes receiving network packets handled by a network entity and building at least one long-term and a least one short-term statistical profile from a measure of the network packets that monitors data transfers, errors, or network connections. A comparison of the statistical profiles is used to determine whether the difference between the statistical profiles indicates suspicious network activity".

Porras is concerned with a "comparison of the statistical profiles," not with packet stream comparison. Thus claims 1-20 are allowable over Porras.

5. As for claim 1, US 615 discloses: A communications monitoring system comprising: a communications sensor for receiving and monitoring in real time communications packets flowing at arbitrary points on a network, said communications being any of communications conducted via a host and communications conducted directly; and a similarity calculator for calculating formal similarity between two packet streams composed of communications packets entering the sensor upon arrival of the communications packets and said sensor employing said formal similarity in detecting an intrusion. (see column 1. line 52, 56 - 61; column 5, lines 46 - 50,58 - 61; Abstract).

In response, the applicants respectfully states that exception is taken with the alleged equivalence of the element of claim 1 and Porras. Claim 1 as amended reads:

1. A communications monitoring system comprising:

a communications sensor for receiving and monitoring in real time communications packets flowing at arbitrary points on a network, said communications being any of communications conducted via a host and communications conducted directly; and

a similarity calculator for calculating formal similarity between two packet streams of similar duration composed of communications packets entering the sensor upon arrival of the communications packets, and said sensor employing said formal similarity in detecting an intrusion.

Thus claim 1 is a communications monitoring system monitoring in real time communications packets flowing at arbitrary points on a network.. Porras is not real time monitoring. Porras is certainly not concerned with any formal similarity between two packet streams of similar duration. As stated above Claim 1 has nothing to do with:

comparison of short and long term anything;

statistical profiles of anything;

generation any statistical score;

any statistical similarities between packet streams;

any network surveillance of short and long term statistical profiles; or

aid in the generation of a statistical score that represents the similarities between the identified network packet streams that were subjected to network surveillance, as in Porras.

Applicants maintain Porras does not teach, have structure for or anticipate:

doing anything at arbitrary points on a network;

doing anything with packet streams of similar duration;

calculating any formal similarity;

any similarity between two packet streams of similar duration;

receiving and monitoring in real time communications packets flowing at arbitrary points on a network;

communications being any of communications conducted via a host and communications conducted directly;

\ calculating formal similarity between anything;

calculating formal similarity between two packet streams composed of communications packets entering the sensor upon arrival of the communications packets;

employing said formal similarity for anything; or

employing said formal similarity in detecting an intrusion.

The referenced portions of Porras column 1, Line 52, 56 - 61; column 5, lines 46-50, 58-61; Abstract) read as follows:.

column 1, Line 52, 56 - 61 reads:
In general, in one aspect, a method of network surveillance includes receiving network packets (e.g., TCP/IP packets) handled by a network entity and building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets that monitors data transfers, errors, or network connections. A comparison of at least one long-term and at least one short-term statistical profile is used to determine whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.

Thus Porras is "building at least one long-term and at least one short-term statistical profile," and performs "comparison of at least one long-term and at least one short-term statistical profile," and determines whether the "difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity." This has no likeness to claim 1, which is

monitoring "in real time" and does "calculating formal similarity between two packet streams. Claim 1 is a packet stream-to packet stream comparison. There is no statistics used in claim 1.

Porras doesn't allude to or anticipate "communications being any of communications conducted via a host and communications conducted directly." Porras doesn't allude to or anticipate "calculating formal similarity between two packet streams." Porras doesn't allude to or anticipate "a communications sensor for receiving and monitoring in real time communications packets flowing at arbitrary points on a network, said communications being any of communications conducted via a host and communications conducted directly." Porras doesn't allude to or anticipate "calculating formal similarity between two packet streams composed of communications packets entering the sensor upon arrival of the communications packets, and said sensor employing said formal similarity in detecting an intrusion. Thus Porras doesn't anticipate claim 1, and claim 1 and claims 2 and 3 that depend on it are allowable.

> *For claim 2, US '615 discloses: The communications monitoring system according to claim 1, wherein the similarity calculator represents the two packet streams by graphs depicting amounts of data in communications packets in respective packet streams with respect to elapsed time, and calculates similarity between the two packet streams based on size of regions enclosed by the two graphs when the graphs of the packet streams are moved close to each other without intersecting each other (see column 6 lines 7 - 15).*

In response, the applicants respectfully states that exception is taken with the alleged equivalence of the element of claim 2 and Porras. Claim 2 is in regard to "two packet streams by graphs depicting amounts of data in communications packets in respective packet streams with respect to elapsed time, and calculates similarity between the two packet streams." Porras is based on statistics, and does not use and is not based on packet streams.

Exception is taken with the so called equivalence of Porras's profiles to graphs. Indeed. a review of the office communication's statement of Porras's "network packet observation and collection (see column 1, lines 51 - 53)" have no teaching of the elements of claim 2.

The further office communication statement, "[M]oreover, the short and long term profiles of Porras are equivalent to the graphs depicting data communications since the profiles consist of data communication information (see column 1, lines 53 - 61; column 2, lines 49-60), is extremely not understood and traversed by the applicants. There is no such equivalence. Porras's profiles, not being graphic cannot be teaching any part of claim 2, and certainly not "calculates similarity between the two packet streams based on size of regions enclosed by the two graphs when the graphs of the packet streams are moved close to each other without intersecting each other." How do profiles move close to each other without intersecting each other?" There is indeed no similarity or parallel teaching in Porras and the graph of claim 2.

Thus Porras doesn't anticipate claim 2, and claim 2 is allowable over Porras for itself and because it depends on an allowable claim.

> *For claim 3 US '615 discloses: The communications monitoring system according to claim 1, wherein the communications sensor sends out a predetermined alert according to a similarity value calculated by the similarity calculator. (see column 4, lines 64 - 66; column 8, lines 23 - 39, 57 - column 9, lines 1 - 5).*

In response, the applicants respectfully states that exception is taken with the alleged equivalence of the element of claim 3 and Porras. The referenced portions of Porras column 4 lines 64-68; column 8, lines 23-39. 57 - column 9, lines 1 -5) read as follows:

column 4 lines 64-68
Referring to FIG. 2, each monitor 16 includes one or more analysis engines 22, 24. These engines 22, 24 can be dynamically added, deleted, and modified as necessary. In the dual-analysis configuration shown, a monitor 16 instantiation includes a signature analysis engine 22 and a statistical profiling engine 24. In general, a monitor 16 may include additional analysis engines that may implement other forms of analysis. A monitor 16 also includes a resolver 20 that implements a response policy and a resource object 32 that configures the monitor 16. The monitors 16 incorporate an application programmers' interface (API) that enhances encapsulation of monitor functions and eases integration of third-party intrusion-detection tools 28, 30.

column 8, lines 23-39,
The analysis engines 22, 24 receive large volumes of events and produce smaller volumes of intrusion or suspicion reports that are then fed to the resolver 20. The resolver 20 is an expert system that receives the intrusion and suspicion reports produced by the analysis engines 22, 24 and reports produced externally by other analysis engines to which it subscribes. Based on these

reports, the resolver 20 invokes responses. Because the volume of intrusion and suspicion reports is lower than the volume of events received by the analysis engines 22, 24, the resolver 20 can afford the more sophisticated demands of configuration maintenance and managing the response handling and external interfaces necessary for monitor operation. Furthermore, the resolver 20 adds to extensibility by providing the subscription interface through which third-party analysis tools 28, 30 can interact and participate in the hierarchical analysis scheme.

57
In addition to external-interface responsibilities, the resolver 20 operates as a fully functional decision engine, capable of invoking real-time response measures in response to malicious or anomalous activity reports produced by the analysis engines. The resolver 20 also operates as the center of intramonitor communication. As the analysis engines 22, 24 build intrusion and suspicion reports, they propagate these reports to the resolver 20 for further correlation, response, and dissemination to other monitors 16a-16f. The resolver 20 can also submit runtime configuration requests to the analysis engines 22, 24, for example, to increase or decrease the scope of analyses (e.g., enable or disable additional signature rules) based on various operating metrics. These configuration requests could be made as a result of encountering other intrusion reports from other subscribers. For example, a report produced by a service monitor 16a-16c in one domain could be propagated to an enterprise monitor 16f, which in turn sensitizes service monitors in other domains to the same activity.

These are not concerned with claim 3 based on packet streams. Porras is based on statistics, and does not use and is not based on packet streams of the same duration. Thus Porras doesn't anticipate claim 3, and claim 3 is allowable over Porras for itself and because it depends on an allowable claim.

> *As for claim 4 US '615 discloses: A communications monitoring system comprising: a packet input means for receiving communications packets flowing at arbitrary points on a network, said communications being any of communications conducted via a host and communications conducted directly; and matching means for performing real-time matching between two packet streams composed of communications packets received by the packet input means and employing said real-time matching in detecting an intrusion. (see column 1, line 52, 56 - 61; column 5, lines 46 - 50, 58 - 61: Abstract).*

In response, the applicants respectfully states that exception is taken with the alleged equivalence of the element of claim 4 and Porras. Claim 4 is a communications monitoring system monitoring in real time communications packets flowing at arbitrary points on a network.. Porras is not real time monitoring.

The referenced portion of Porras are not concerned with anything at arbitrary points as in the elements of claim 4. These Porras portions column 1, line 52, 56- 61; column 5, lines 46 -50, 58 - 61; Abstract) read as above and as follows.

column 1, Line 52, 56 - 61
In general, in one aspect, a method of network surveillance includes receiving network packets (e.g., TCP/IP packets) handled by a network entity and building at least one long-term and at least one short-term statistical profile from at least one measure of the network packets that monitors data transfers, errors, or network connections. A comparison of at least one long-term and at least one short-term statistical profile is used to determine whether the difference between the short-term statistical profile and the long-term statistical profile indicates suspicious network activity.

Embodiments may include one or more of the following features. The measure may monitor data transfers by monitoring network packet data transfer commands, data transfer errors, and/or monitoring network packet data transfer volume. The measure may monitor network connections by monitoring network connection requests, network connection denials, and/or a correlation of network connections requests and network connection denials. The measure may monitor errors by monitoring error codes included in a network packet such as privilege error codes and/or error codes indicating a reason a packet was rejected.

column 5, lines 46-50, 58-61
The profile engine 22 can use a wide range of multivariate statistical measures to profile network activity indicated by an event stream. A statistical score represents how closely currently observed usage corresponds to the established patterns of usage. The profiler engine 22 separates profile management and the mathematical algorithms used to assess the anomaly of events. The profile engine 22 may use a statistical analysis technique described in A. Valdes and D. Anderson, "Statistical Methods for Computer Usage Anomaly Detection Using NIDES", Proceedings of the Third International Workshop on Rough Sets and Soft Computing, January 1995, which is incorporated by reference in its entirety. Such an engine 22 can profile network activity via one or more variables called measures. Measures can be categorized into four classes: categorical, continuous, intensity, and event distribution measures.

Categorical measures assume values from a discrete, nonordered set of possibilities. Examples of categorical measures include network source and destination addresses, commands (e.g., commands that control data transfer and manage network connections), protocols, error codes (e.g., privilege violations, malformed service requests, and malformed packet codes), and port identifiers. The profiler engine 22 can build empirical distributions of the category values encountered, even if the list of possible values is open-ended. The engine 22 can have mechanisms for "aging out" categories whose long-term probabilities drop below a threshold.

Thus claim 4 is a communications monitoring system monitoring in real time communications packets flowing at arbitrary points on a network. Porras is not real time monitoring of arbitrary

points. Porras is based on packet statistics. Porras doesn't allude to or anticipate "communications being any of communications conducted via a host and communications conducted directly." Porras doesn't allude to or anticipate "packet streams." Porras doesn't allude to or anticipate "performing real-time matching between two packet streams composed of communications packets received by the packet input means." Porras doesn't allude to or anticipate "employing said real-time matching in detecting an intrusion." Thus Porras doesn't anticipate claim 4, and claim 4 and claims 5 and 6 that depend on it are allowable.

For claim 5, US '615 discloses: The communications monitoring system according to claim 4, wherein the matching means determines formal similarity between the two packet streams based on a time lag between each corresponding pair of communications packets in the two packet streams. (see column 6, lines 7 - 15).

In response, the applicants respectfully states that exception is taken with the alleged equivalence of the element of claim 5 and Porras. Porras is not concerned with matching packet streams. Porras is based on long and short term statistics. Porras fails to show matching means determines formal similarity between the two packet streams based on a time lag between each corresponding pair of communications packets in the two packet streams. Claim 5 is amended and includes "formal similarity between the two packet streams being similar in an amount of data and transmission interval of packets irrespective of data content and is determined based on a time lag between each corresponding pair of communications packets in the two packet streams." There is no such teaching in Porras. Thus Porras doesn't anticipate claim 5, and claim 5 is allowable over Porras for itself and because it depends on an allowable claim.

For claim 6, US '615 discloses: The communications monitoring system according to claim 5, further comprising alerting means for sending out a predetermined alert according to the formal similarity between the two packet streams determined by the matching means. (see column 4, lines 64 - 66; column 8, lines 23 - 39, 57 - column 9, lines 1 - 5).

In response, the applicants respectfully states that exception is taken with the alleged equivalence of the element of claim 6 and Porras. Referenced portions of Porras are not concerned with Claim 6. Porras column 4, lines 64-86; column 8, Lines 23- 39, 57 -column 9, lines 1 -5) read:

column 4 lines 64-68
Referring to FIG. 2, each monitor 16 includes one or more analysis engines 22, 24. These engines 22, 24 can be dynamically added, deleted, and modified as necessary. In the dual-analysis configuration shown, a monitor 16 instantiation includes a signature analysis engine 22 and a statistical profiling engine 24. In general, a monitor 16 may include additional analysis engines that may implement other forms of analysis. A monitor 16 also includes a resolver 20 that implements a response policy and a resource object 32 that configures the monitor 16. The monitors 16 incorporate an application programmers' interface (API) that enhances encapsulation of monitor functions and eases integration of third-party intrusion-detection tools 28, 30.
In addition to external-interface responsibilities, the resolver 20 operates as a fully functional decision engine, capable of invoking real-time response measures in response to malicious or anomalous activity reports produced by the analysis engines. The resolver 20 also operates as the center of intramonitor communication. As the analysis engines 22, 24 build intrusion and suspicion reports, they propagate these reports to the resolver 20 for further correlation, response, and dissemination to other monitors 16a-16f. The resolver 20 can also submit runtime configuration requests to the analysis engines 22, 24, for example, to increase or decrease the scope of analyses (e.g., enable or disable additional signature rules) based on various operating metrics. These configuration requests could be made as a result of encountering other intrusion reports from other subscribers. For example, a report produced by a service monitor 16a-16c in one domain could be propagated to an enterprise monitor 16f, which in turn sensitizes service monitors in other domains to the same activity.

This is not claim 6's "alerting means for sending out a predetermined alert according to the formal similarity between the two packet streams determined by the matching means." Thus Porras doesn't anticipate claim 6, and claim 6 is allowable over Porras for itself and because it depends on an allowable claim.

As for claim 7, US '615 discloses: A communications monitoring method for monitoring data communications using a computer, comprising the steps of: acquiring in real time communications packets in sequence from arbitrary points on a network and storing them in predetermined storage means together with information about a packet stream to which the communications packets belong, said communications being any of communications conducted via a host and communications conducted directly; on reception of a predetermined communication packet, taking another communications packet received within a predetermined time before acquiring a predetermined communications packet, out of the storage means; determining formal similarity between the first packet stream which contains up to the acquired communications packet and a

second packet stream to which the communications packet taken out of the storage means belong: and sending out a predetermined alert according to the determined similarity. (see column 1, line 52, 56 - 61; column 5, lines 46 - 50, 58 - 61; Abstract).

In response, the applicants respectfully states that exception is taken with the alleged equivalence of the element of claim 7 and Porras. Claim 7 is amended to read:

7. (Currently amended) A communications monitoring method for monitoring data communications using a computer, comprising the steps of:

acquiring in real time communications packets in sequence from arbitrary points on a network and storing them in predetermined storage means together with information about a packet stream to which the communications packets belong, said communications being any of communications conducted via a host and communications conducted directly;

on reception of a predetermined communication packet, taking another communications packet received within a predetermined time before acquiring a predetermined communications packet, out of the storage means;

determining formal similarity between the first packet stream which contains up to the acquired communications packet and a second packet stream to which the communications packet taken out of the storage means belong; and

sending out a predetermined alert according to the determined similarity.

Porras is not concerned with matching packet streams. Porras is based on long and short term statistics. Porras fails to show "formal similarity between the first packet stream."

Porras doesn't allude to or anticipate "acquiring in real time communications packets in sequence."

Porras doesn't allude to or anticipate first and second packet streams "being of similar duration of said first packet stream.

Porras doesn't allude to or anticipate storing "in predetermined storage means together with information about a packet stream to which the communications packets belong."

Porras doesn't allude to or anticipate "communications being any of communications conducted via a host and communications conducted directly.

Porras doesn't allude to or anticipate "reception of a predetermined communication packet, taking another communications packet received within a predetermined time before acquiring a predetermined communications packet, out of the storage means."

Porras doesn't allude to or anticipate "determining formal similarity between the first packet stream which contains up to the acquired communications packet and a second packet stream to which the communications packet taken out of the storage means belong."

Porras doesn't allude to or anticipate "sending out a predetermined alert according to the determined similarity."

Thus Porras doesn't anticipate claim 7, and claim 7 and claims 8 and 9 that depend on it are allowable.

For claim 8, US '615 teaches: The communications monitoring method according to claim 7, wherein in the step of determining the formal similarity of packet streams, the formal similarity between the two packet streams is determined based on a time lag between each corresponding pair of communications packets in the two packet streams. (see column 6, lines 7 - 15).

In response, the applicants respectfully states that exception is taken with the alleged equivalence of the element of claim 9 and Porras. Porras column 6 Lines 7 - 15 portion reads as follows:

column 6 Lines 7 - 15
Continuous measures assume values from a continuous or ordinal set. Examples include inter-event time (e.g., difference in time stamps between consecutive events from the same stream), counting measures such as the number of errors of a particular type observed in the recent past, the volume of data transfers over a period of time, and network traffic measures (number of packets and number of kilobytes). The profiler engine 22 treats continuous measures by first allocating bins appropriate to the range of values of the underlying measure, and then tracking the frequency of observation of each value range. In this way, multi-modal distributions are accommodated and much of the computational machinery used for categorical measures is shared. Continuous measures are useful not only for intrusion detection, but also to support the monitoring of the health and status of the network from the perspective of connectivity and throughput. For example, a measure of traffic volume maintained can detect an abnormal loss in the data rate of received packets when this volume falls outside historical norms. This sudden drop can be specific both to the network entity being monitored and to the time of day (e.g., the average sustained traffic rate for a major network artery is much different at 11:00 a.m. than at midnight).

This is not relevant to or teach elements Claim 8. Porras is not concerned with matching packet streams. Porras is based on long and short term statistics. Porras fails to show matching means determines formal similarity between the two packet streams based on a time lag between each corresponding pair of communications packets in the two packet streams. Thus Porras doesn't anticipate claim 8, and claim 8 is allowable over Porras for itself and because it depends on an allowable claim.

For claim 9, US '615 teaches: The communications monitoring method according to claim 7, further comprising a step of discarding information used in determining the similarity of second packet streams except the second packet stream determined to be most similar to the first packet stream. (see column 6, lines 7 - 15; column 8, lines 23 - 39. 57 - column 9, lines 1 - 5).

In response, the applicants respectfully states that exception is taken with the alleged equivalence of the element of claim 9 and Porras. A review of the referenced portions of Porras show that Porras is not concerned with Claim 9. Porras is not concerned with "discarding information used in determining the similarity of second packet streams except the second packet stream determined to. be most similar to the first packet stream." Thus Porras doesn't anticipate claim 9, and claim 9 is allowable over Porras for itself and because it depends on an allowable claim.

> *As for claim 10 US '615 teaches: An information processing method comprising comparing two packet streams flowing in real time on a network, the step of comparing comprising the steps of. acquiring communications packets in sequence from arbitrary points on a network and storing them in predetermined storage means together with information about a packet stream to which the communications packets belong, said communications packets being in any of communications conducted via a host and communications conducted directly; on reception of a predetermined communication packet, taking another communications packet received within a predetermined time before acquiring a predetermined communications packet, out of the storage means; and performing matching between the first packet stream which contains up to the acquired communications packet and a second packet stream to which the communications packet taken out of the storage means belong. (see column 1, line 52, 56 - 61; column 5,. lines 46 - 50, 58 - 61; Abstract).*

In response, the applicants respectfully states that exception is taken with the alleged equivalence of the element of claim 10 and Porras. Claim 10 reads

> 10. An information processing method comprising comparing two packet streams flowing in real time on a network, the step of comparing comprising the steps of:
>
> acquiring communications packets in sequence from arbitrary points on a network and storing them in predetermined storage means together with information about a packet stream to which the communications packets belong, said communications packets being in any of communications conducted via a host and communications conducted directly;

on reception of a predetermined communication packet, taking another communications packet received within a predetermined time before acquiring a predetermined communications packet, out of the storage means; and

performing matching between the first packet stream which contains up to the acquired communications packet and a second packet stream to which the communications packet taken out of the storage means belong.

As with independent claims 1, 4 and 7, claim 10 is not anticipated by Porras. Porras is based on statistics. Thus, Porras doesn't allude to or anticipate "comparing two packet streams." Porras doesn't allude to or anticipate these "flowing in real time on a network.

Porras doesn't allude to or anticipate "acquiring communications packets in sequence from arbitrary points on a network and storing them in predetermined storage means together with information about a packet stream to which the communications packets belong."

Porras doesn't allude to or anticipate "packets being in any of communications conducted via a host and communications conducted directly."

Porras doesn't allude to or anticipate "reception of a predetermined communication packet, taking another communications packet received within a predetermined time before acquiring a predetermined communications packet, out of the storage means."

Porras doesn't allude to or anticipate "performing matching between the first packet stream which contains up to the acquired communications packet and a second packet stream to which the communications packet taken out of the storage means belong."

Porras doesn't allude to or anticipate a "second packet stream being of similar duration of said first packet stream.

Thus, Porras doesn't anticipate claim 10, and claims 11 and 12 are allowable over Porras each for itself and/or because it depends on an allowable claim.

> *For claim 11, US '615 teaches: The information processing method according to claim 10, wherein in the step of performing matching between the packet streams, the first and second packet streams are represented by graphs which depict increments of sequence numbers of communications packets in respective packet streams with respect to elapsed time and the similarity between the two packet streams is calculated based on size of regions enclosed by the two graphs when the graphs of the packet streams are moved close to each other without intersecting each other. (see column 6, lines 7 - 15).*

In response, the applicants respectfully states that exception is taken with the alleged equivalence of the element of claim 11 and Porras. A review of the copied portions of Porras show that Claim 11 is not anticipated by Porras and is allowable over Porras for itself and because it depends on an allowable claim.

> *For claim 12, US '615 teaches: The information processing method according to claim 11, wherein in the step of calculating the similarity between the packet streams, information used n determining the similarity is discarded according to time-axis lengths of the regions enclosed by the two graphs. (see column 6, lines 7 - 15; column 8, lines 23 - 39.57 - column 9, lines 1 - 5).*

In response, the applicants respectfully states that exception is taken with the alleged equivalence of the element of claim 12 and Porras. A review of the copied portions of Porras show that Claim

12 is not anticipated by Porras and is allowable over Porras for itself and because it depends on an allowable claim.

For claim 13, US 615 teaches: An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing communications monitoring, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 7. (see Figure 6).

For claim 14, US '615 teaches: A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for communications monitoring, said method steps comprising the steps of claim 7. (see Figure 6).

For claim 15, US '615 teaches: An article of manufacture comprising a computer usable medium having computer readable program code means embodied therein for causing information processing, the computer readable program code means in said article of manufacture comprising computer readable program code means for causing a computer to effect the steps of claim 10. (see Figure 6).

For claim 16, US 615 teaches: A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for information processing, said method steps comprising the steps of claim 10. (see Figure 6).

For claim 17, US '615 teaches: A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing communications monitoring, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 1. (see column 2, lines 32 - 36; Figure 6).

For claim 18, US '615 teaches: A computer program product comprising a computer usable medium having computer readable program code means embodied therein for causing communications monitoring, the computer readable program code means in said computer program product comprising computer readable program code means for causing a computer to effect the functions of claim 4. (see column 2, lines 32 - 36; Figure 6).

In response, the applicants respectfully states that exception is taken with the alleged equivalence of the element of claims 13- 18 and Porras. Claims 13-18 are computer and Beauregard claims

not anticipated by Porras. Thus Porras doesn't anticipate claims 13-18 which are allowable over Porras each for itself and because it depends on an allowable claim.

> *For claim 19, US '615 teaches: the communications monitoring system according to Claim 1, wherein the similarity calculator represents the two packet streams by graphs depicting amounts of data in communications packets in respective packet streams with respect to elapsed time, and calculates similarity between the two packet streams based on size of regions enclosed by the two graphs when the graphs of the packet streams are moved close to each other without intersecting each other, (see column 6, lines 7 - 15) and wherein the communications sensor sends out a predetermined alert according to a similarity value calculated by the similarity calculator.((see column 4, lines 64 - 66; column 8, lines 23 - 39, 57 - column 9, lines 1 -5).*

In response, the applicants respectfully states that as was shown for claims 1 and 2, Porras indeed fails to teach "the communications monitoring system according to Claim 1." A review of Porras column 6, lines 7 - 15, shows that Porras fails to teach or anticipate any graph, any formal similarity, any calculation of a formal similarity. and certainly fails to teach "wherein the communications sensor sends out a predetermined alert according to a similarity value calculated by the similarity calculator in Porras column 4, lines 64 - 66; column 8, lines 23 - 39, 57 - column 9, lines 1 -5.

Thus, Claim 19 is not anticipated by Porras and is allowable over Porras for itself and because it depends on an allowable claim.

> *For claim 20, US 615 teaches: The information processing method according to Claim 10, wherein in the step of performing matching between the packet streams, the first and second packet streams are represented by graphs which depict increments of sequence numbers of communications packets in respective packet streams with respect to elapsed time and the similarity between the two packet streams is calculated based on size of regions enclosed by the two graphs when the graphs of the packet streams are moved close to each other without intersecting each other, (see column 6, lines 7 - 15) and wherein in the step of calculating the similarity between the packet streams, information used in determining the similarity is discarded according to time-axis lengths of the regions enclosed by the two graphs (see column 6, lines 7 -15; column 8, lines 23 - 39,57 - column 9, lines 1 - 5).*

In response, the applicants respectfully states that as was shown for claims 1 and 2, Porras indeed fails to teach "the information processing method according to Claim 10." A review of Porras

column 6, lines 7 - 15, and column 4, lines 64 - 66; column 8, lines 23 - 39, 57 - column 9, lines 1 -5, shows that Porras fails to teach or anticipate any graph, anything like a "step of performing matching between the packet streams, the first and second packet streams are represented by graphs which depict increments of sequence numbers of communications packets in respective packet streams with respect to elapsed time and the similarity between the two packet streams is calculated based on size of regions enclosed by the two graphs when the graphs of the packet streams are moved close to each other without intersecting each other, and Porras fails to teach or anticipate any graph, anything like a "step of calculating the similarity between the packet streams, information used in determining the similarity is discarded according to time-axis lengths of the regions enclosed by the two graphs." Thus, Claim 20 is not anticipated by Porras and is allowable over Porras for itself and because it depends on an allowable claim.

It is anticipated that this brings allowance of claims 1-20. Please contact the undersigned if any question remains. Please charge any fee necessary to enter this paper to deposit account 50-0510.

Respectfully submitted,

By: _____/Louis Herzberg/____
Dr. Louis P. Herzberg
Reg. No. 41,500
Voice Tel. (845) 352-3194
Fax. (845) 352-3194
3 Cloverdale Lane
Monsey, NY 10952

Customer Number: 54856